

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

DICE CORPORATION,

Plaintiff,

v.

Case Number 11-13578
Honorable Thomas L. Ludington

BOLD TECHNOLOGIES,

Defendant.

_____ /

OPINION AND ORDER DENYING DEFENDANT’S MOTION TO DISMISS

This intellectual property dispute presents a somewhat unusual question of statutory interpretation: Is an “and” disjunctive? The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, creates a civil cause of action against a person who accesses a protected computer without authorization and causes “loss to 1 or more persons . . . aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(I); *id.* § 1030(g) (creating private cause of action).

Plaintiff Dice Corporation alleges that one of its employees left, took a job with a competitor, Defendant Bold Technologies, and then accessed data on Plaintiff’s computers. Plaintiff investigated, added security, and sued Defendant. Among its claims, Plaintiff asserted a violation of the Act. Defendant now moves to dismiss the claim, asserting that Plaintiff does not allege a “loss” within the meaning of the Act because it does not allege an “interruption of service.” ECF No. 21. Plaintiff responds such an allegation is unnecessary as a particular “and” in the Act’s definition of “loss” is disjunctive. In pertinent part, the Act provides that

the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, *and* any

revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11) (emphasis added). Under Plaintiff's interpretation, the "and" is disjunctive. Thus, the provision at issue should be read to convey:

the term "loss" means any reasonable cost to any victim, including the cost of
[A] responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and
[B] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. Under Defendant's interpretation, in contrast, the "and" is not disjunctive. Thus, the provision should be read as:

the term "loss" means any reasonable cost to any victim, including the cost of
[A] responding to an offense,
[B] conducting a damage assessment, and
[C] restoring the data, program, system, or information to its condition prior to the offense, and
[D] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. Since "because of interruption of service" modifies each of the foregoing clauses, Defendant contends, "loss" requires interruption of service.

Both parties' interpretations, it must be acknowledged, are reasonable. As yet no appellate court has expressly addressed the issue. *See Cont'l Grp., Inc. v. KW Prop. Mgmt.*, 622 F. Supp. 2d 1357, 1371 (S.D. Fla. 2009). District courts, moreover, have reached different conclusions. *Compare Quantlab Techs. Ltd. v. Godlevsky*, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010) ("[T]he term 'loss' encompasses . . . two types of harm: costs to investigate and respond to a computer intrusion, and costs associated with a service interruption."), *with Gen. Scientific Corp. v. SheerVision*, No. 10-cv-13582, 2011 WL 3880489, at *4 (E.D. Mich. Sept. 2, 2011) (Rosen, C.J.) ("The CFAA only covers lost revenue if the loss occurred as a result of interrupted

service.”), and *Cont’l Grp.*, 622 F. Supp. 2d at 1371 (“[A]ll loss must be as a result of ‘interruption of service.’”).

The legislative history, however, suggests that Plaintiff has the better argument. As initially proposed, the bill that later became law provided:

the term “loss” includes—

(A) the reasonable costs to any victim of—

(i) responding to the offense;

(ii) conducting a damage assessment; and

(iii) restoring the system and data to their condition prior to the offense; and

(B) any lost revenue or costs incurred by the victim as a result of interruption of service.

Enhancement of Privacy and Public Safety in Cyberspace Act, S. 3083, 106th Cong. (2000), *quoted in DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 522 n.29 (S.D.N.Y. 2001).

Although this internal structure was omitted from the definition enacted the following year, it strongly suggests that the drafters did intend that “loss” embrace two types of injury. Colloquially, the “and” means “or.” Accordingly, the Court will deny Defendant’s motion.

I

Plaintiff, a Michigan corporation, provides security monitoring services, which involves remote monitoring of fire alarms, burglar alarms, and other security devices at client sites. Defendant, an Illinois corporation, is a competitor providing similar services. On May 27, 2011, one of Plaintiff’s employees, Amy Condon, left Plaintiff’s employment and joined Defendant’s firm. Over the next two weeks, Plaintiff alleges, Ms. Condon accessed “servers located in [Plaintiff’s] Bay City facility . . . that contained proprietary signal processing intelligence software.” Second Am. Compl. ¶ 12, ECF No. 20. Over the following two weeks, Plaintiff further alleges, Ms. Condon accessed “servers located at client sites and initiated file transfers of proprietary signal processing intelligence software.” *Id.*

In August 2011, Plaintiff brought suit against Defendant, asserting claims for violations of Michigan's Uniform Trade Secrets Act, conversion, and unjust enrichment. In October, Plaintiff filed its first amended complaint, adding claims for violations of the Act, the Digital Millennium Copyright Act, and copyright infringement.

In pertinent part, the claim for violation of the Act alleged simply that Plaintiff "has sustained damages as a result of [Defendant's] violation of this Act." First Am. Compl. ¶¶ 38–40, ECF No. 14. Defendant moved to dismiss the first amended complaint in part. Regarding the claimed violation of the act, Defendant asserted it should be dismissed "because [Plaintiff] alleges no facts showing that it sustained a 'loss' within the meaning of 18 U.S.C. § 1030(e)(11)." Def.'s Mot. to Dismiss ¶ 3, ECF No. 17.

In November 2011, the Court entered a stipulated order permitting Plaintiff to file a second amended complaint. In pertinent part, the order permitted Plaintiff to revise its claimed losses under the Act. ECF No. 19. Plaintiff did so, alleging in pertinent part:

[Plaintiff] has sustained a "loss" significantly in excess of \$5,000 as a result of [Defendant's] violation of this Act. Specifically, [Plaintiff] has incurred and continues to incur costs attributable to damage assessment and remedial activities necessary to terminate Defendant's unauthorized access to [Plaintiff's] servers.

Second Am. Compl. ¶ 34. Defendant now moves to dismiss the claimed violation of the Act, again asserting it should be dismissed because it "lacks adequate factual allegations to demonstrate that [Plaintiff] sustained a covered 'loss' within the meaning of 18 U.S.C. § 1030(e)(11)." Def.'s Mot. to Dismiss Second Am. Compl. 1, ECF No. 21.

II

Federal Rule of Civil Procedure 12(b)(6) requires that a court dismiss a claim if it does not "state a claim upon which relief can be granted." To survive a Rule 12(b)(6) motion to dismiss, the complaint "must contain sufficient factual matter, accepted as true, to state a claim

to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009) (internal quotation marks omitted) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

III

A

“The starting point for interpretation of a statute is the language of the statute itself.” *Kaiser Aluminum & Chem. Corp. v. Bonjorno*, 494 U.S. 827, 835 (1990) (internal quotation marks and citation omitted). As the Supreme Court explains: “Our first step in interpreting a statute is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case. Our inquiry must cease if the statutory language is unambiguous.” *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340–41 (1997). “If the language of the statute is clear, a court must give effect to this plain meaning.” *Broadcast Music, Inc. v. Roger Mills Music, Inc.*, 396 F.3d 762, 769 (6th Cir. 2005) (citing *Barnhart v. Sigmon Coal, Inc.*, 534 U.S. 438, 451 (2002)).

If the language of the statute is ambiguous, however, the court must consider “extrinsic material” to determine its meaning. *Oklahoma v. New Mexico*, 501 U.S. 221, 235 n.5 (1991) (“[W]e repeatedly have looked to legislative history and other extrinsic material when required to interpret a statute which is ambiguous.”). “The primary rule of statutory construction is to ascertain and give effect to the legislative intent.” *Hedgepeth v. Tennessee*, 215 F.3d 608, 616 (6th Cir. 2000). Consequently, the Sixth Circuit instructs, in interpreting an ambiguous term “it is our duty to examine the legislative history in order to render an interpretation that gives effect to Congress’s intent.” *United States v. Markwood*, 48 F.3d 969, 975 n.7 (6th Cir. 1995) (citing *In re Vause*, 886 F.2d 794, 801 (6th Cir.1989)).¹

¹ This “duty,” it should be observed, is not universally acknowledged outside the Sixth Circuit. Compare Antonin Scalia, *A Matter of Interpretation* 29–37 (1997) (criticizing the use of legislative history), with Stephen

In this case, as noted, the language of the statute does not unequivocally establish whether the “and” is disjunctive or not. One reasonable interpretation is:

- the term “loss” means any reasonable cost to any victim, including
- [A] the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and
 - [B] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). An equally reasonable interpretation, however, is:

- the term “loss” means any reasonable cost to any victim, including the cost of
- [A] responding to an offense,
 - [B] conducting a damage assessment, and
 - [C] restoring the data, program, system, or information to its condition prior to the offense, and
 - [D] any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

In sum, as another district court observed when confronted with this issue, “reasonable minds surely can differ until the Court of Appeals decides the issue.” *Cont’l Grp.*, 622 F. Supp. 2d at 1371. Therefore, it is this Court’s duty to consult the legislative history of the Act. *Markwood*, 48 F.3d at 975 n.7.

B

The Act, the “first Federal computer crime statute,” S. Rep. 104–357, at 3 (1996), had its genesis in the enactment of “a massive omnibus crime bill known as the Comprehensive Crime Control Act [of 1984, Pub. L. No. 98–473, 98 Stat. 1976].” Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1563 (2010).

Breyer, *Making Our Democracy Work* 92–102 (2010) (endorsing the use of legislative history). See generally Michael H. Koby, *The Supreme Court’s Declining Reliance on Legislative History: The Impact of Justice Scalia’s Critique*, 36 Harv. J. on Legis. 369, 370 (1999) (producing an empirical study on the Supreme Court’s use of legislative history from 1980 to 1998 and concluding “that there has been a significant decrease in the Supreme Court’s reliance on legislative history documents, attributable at least in part to Justice Scalia’s criticism of its use”).

Codified at 18 U.S.C. § 1030, it criminalized “three specific [actions]: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers.” *Id.* at 1564 (citing 18 U.S.C. § 1030(a)(1)–(3)).

Two years later, Congress formally introduced the Act with enactment of the Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213. Amending § 1030, Congress created three more computer crimes:

Section 1030(a)(4) prohibited unauthorized access with intent to defraud; essentially, the traditional crime of wire fraud committed using a computer. Section 1030(a)(5) prohibited accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either \$1,000 or more of aggregated loss Section 1030(a)(6) prohibited trafficking in computer passwords.

Kerr, *supra*, at 1565 (footnotes omitted). The legislative history explains that the amendments were necessary because of a “technological explosion,” elaborating:

In 1978, there were an estimated 5,000 desk-top computers in this country; today there are nearly 5 million. . . . This technological explosion has made the computer a mainstay of our communications system, and it has brought a great many benefits to the government, to American businesses, and to all of our lives. But it has also created a new type of criminal — one who uses computers to steal, to defraud, and to abuse the property of others. The proliferation of computers and computer data has spread before the nation’s criminals a vast array of property that, in many cases, is wholly unprotected against crime. . . .

The new subsection 1030(a)(5) to be created by the bill is designed to . . . penalize alteration, damage, or destruction . . . which cause[s] a loss to the victim or victims totaling \$1,000 or more in any single year period. The Committee believes this threshold is necessary to prevent the bringing of felony-level charges against every individual who modifies another’s computer data. Some modifications or alterations, while constituting “damage” in a sense, do not warrant felony-level punishment, particularly when almost no effort or expense is required to restore the affected data to its original condition. . . .

The Department of Justice has suggested that the concept of “loss” embodied in this subsection not be limited to the costs of actual repairs. The Committee agrees and intends that other expenses accruing to the victim — such as lost computer time and the cost of reprogramming or restoring data to its original condition — be permitted to count toward the \$1,000 valuation. . . .

S. Rep. 99-432, at 1, 10, 11(1986).

Eight years passed. In 1994, Congress enacted another omnibus crime bill, the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796. Although better known for its provisions regarding a federal assault weapons ban, the bill also included the Computer Abuse Amendments Act, which added civil remedies for violations of the section. *See generally* Deborah F. Buckman, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. Fed. 101 (2001) (observing that the Act “provided only criminal penalties until enactment of the Computer Abuse Amendments Act of 1994, which added the civil remedies, 18 U.S.C.A. § 1030(g)”).

“Any person who suffers damage or loss by reason of a violation of the section,” the new subsection (g) provided in pertinent part, “may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g) (1994). The legislative history of an earlier draft of the Act explained: “This remedy [will] authorize private suits in an area that law enforcement has sometimes been reluctant to investigate or prosecute. Deterrence is another goal.” S. Rep. 101-544, at 8 (1990).

In 1996, § 1030 was again amended as part of the Economic Espionage Act of 1996, Pub. L. 104-294, tit. II, 110 Stat. 3488, 3491. In pertinent part, it amended § 1030(a)(5) to create separate offenses for the unauthorized computer access. The legislative history explains:

[U]nder the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.

The rationale for this difference in treatment deserves explanation. Although those who intentionally damage a system, without authority, should be punished regardless of whether they are authorized users, it is equally clear that anyone

who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. . . .

The 1994 amendment required both “damage” and “loss,” but it is not always clear what constitutes “damage.” For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no “damage,” the victim does suffer “loss.” If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief. . . .

The bill also amends the civil penalty provision under section 1030(g) to be consistent with the amendments to section 1030(a)(5).

S. Rep. 104–357, at 10–11 (1995).

In 2000, Senator Patrick Leahy “introduced a bill, the Enhancement of Privacy and Public Safety in Cyberspace Act in the Senate that expressly [sought] to clarify (1) what constitutes ‘loss,’ and (2) that ‘loss’ is subject to the \$5,000 monetary threshold.” *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 522 n.29 (S.D.N.Y. 2001) (internal citation omitted) (citing 146 Cong. Rec. S8823–01 (Sept. 20, 2000)). As initially proposed, the bill provided:

the term “loss” includes—

- (A) the reasonable costs to any victim of—
 - (i) responding to the offense;
 - (ii) conducting a damage assessment; and
 - (iii) restoring the system and data to their condition prior to the offense; and
- (B) any lost revenue or costs incurred by the victim as a result of interruption of service.

Enhancement of Privacy and Public Safety in Cyberspace Act, S. 3083, 106th Cong. (2000), *quoted in In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at n.29; *see also Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004) (same).

The following year, these additions were adopted (with minor modifications) as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272. Section 814 of the act, titled “Deterrence and Prevention of Cyberterrorism,” added the definition of “loss” at issue in this case, providing in pertinent part:

the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. (emphasis added). This definition has not been revised and is currently in force. *See* 18 U.S.C. § 1030(e)(11).

Although the earlier draft’s express separation of loss into two subdivisions — literally, subdivisions “A” and “B” — did not make it into the final bill, nothing suggests that this modification was intended to be substantive. Rather, although minor stylistic changes were made, in substance Senator Leahy’s bill was adopted in full. And unlike the “committee reports,” which are viewed with a particularly jaundiced eye by legislative history skeptics,² this draft is integral to the legislation’s history.

² *See, e.g.,* Scalia, *supra*, at 34 (“Ironically, but quite understandably, the more courts have relied on legislative history, the less worthy of reliance it has become. In earlier days, it was at least genuine and not contrived — a real part of the legislation’s history, in the sense that it was a part of the development of the bill, part of the attempt to inform and persuade those who voted. Nowadays, however, when it is universally known and expected that judges will resort to floor debates and (especially) committee reports as authoritative expressions of ‘legislative intent,’ affecting the courts rather than informing the Congress has become the primary purpose of the exercise. It is less that the courts refer to the legislative history because it exists than that the legislative history exists because the courts refer to it.”).

Turning to the committee reports, they likewise support the conclusion that “loss” does not require “interruption of service.” From the beginning, for example, “the concept of ‘loss’ embodied in this subsection” included “the costs of actual repairs.” S. Rep. 99-432, at 10 (1986). With the amendments in 1996, Congress clarified that it sought to punish — and compensate the victim for — “the intentional act of trespass,” with the legislative history explaining that the trespass “requires the system administrator to devote resources to resecur[ing] the system. Thus, although there is arguably no ‘damage,’ the victim does suffer ‘loss.’ If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.” S. Rep. 104–357, at 10 (1995). Thus, from the beginning, “loss” has been defined broadly to include not only the harm the intruder directly inflicts, but also the costs the victim incurs in investigating and preventing future incursions.

“Interruption of service,” in contrast, does not share this distinguished pedigree. It did not appear in either the legislative history or the proposed text of the Act itself until Senator Leahy’s bifurcated definition of “loss” in 2000, quoted above — in which it is an alternative form of loss. This strongly suggests that the Act’s definition of “loss” is disjunctive. The “and” means “or.”

C

This conclusion, of course, does not square with a recent decision in *General Scientific Corp. v. SheerVision*, No. 10–cv–13582, 2011 WL 3880489 (E.D. Mich. Sept. 2, 2011), in which Chief Judge Rosen reached a different result, writing: “The CFAA only covers lost revenue if the loss occurred as a result of interrupted service.” *Id.* at 4.

Different interpretations of the same statute within the same district court are generally not preferred (except, perhaps, by courts of appeals, which were created in part to resolve such

differences of opinion). Somewhat moderating this difference, however, are two significant factors. First, the interpretation in *SheerVision* was not essential to the disposition of the case — it was offered as an alternative rationale. In pertinent part, the court wrote:

Plaintiff's CFAA claim fails under both the statutory definition of "loss" and *Twombly*.

First, Plaintiff has failed to allege specific facts suggesting the plausibility of damages required under the CFAA. Plaintiff merely "believes that it will incur" costs exceeding \$5,000. A mere belief in purported future damages is insufficient to survive a Rule 12(b)(6) motion because a complaint requires more than labels and conclusions, and "a formulaic recitation of the elements of a cause of action will not do." Plaintiff has not alleged specific facts suggesting that it incurred at least \$5,000 in losses as a result of Defendants' alleged activity.

Second, to the extent Plaintiff has attempted to bolster its pleading through its Response to Defendants' Motion to Dismiss and the affidavit of Gregory S. Smith, Plaintiff demonstrates a misinterpretation of the "loss" standard under the CFAA, further undermining its claim. The crux of Plaintiff's response rests on the contention that Defendants' conduct has caused at least \$5,000 in losses through usurped sales opportunities. Lost sales and profits *per se* are not the measure of loss under the CFAA, however. As the statutory language makes clear, "losses" under the CFAA are limited to costs incurred and profits lost as a direct result of interrupted computer service.

SheerVision, 2011 WL 3880489, at *3–4 (internal citations omitted). Thus, the court first granted the motion to dismiss because the plaintiff had not pled sufficient factual matter to state a claim upon which relief could be granted, offering its interpretation only as an alternative rationale. *But cf. McLellan v. Miss. Power & Light Co.*, 545 F.2d 919, 925 n.21 (5th Cir. 1977) ("It has long been settled that all alternative rationales for a given result have precedential value. 'It does not make a reason given for a conclusion in a case obiter dictum, because it is only one of two reasons for the same conclusion.'" (quoting *Richmond Screw Anchor Co. v. United States*, 275 U.S. 331, 340 (1928))).

Second, the parties did not brief, and so the court did not address, the legislative history of the Act. *See, e.g.*, Plaintiff's Answer to Defendant Sheervision's Motion to Dismiss and Brief in Support at 6–7, *SheerVision*, 2011 WL 3880489 (No. 10–cv–13582), ECF No. 14.

IV

Accordingly, it is **ORDERED** that Defendant's motion to dismiss (ECF No. 21) is denied.

It is further **ORDERED** that the hearing on Defendant's motion scheduled for Tuesday, January 31, 2012, at 4:00 p.m. is cancelled because the parties' papers provide the necessary factual and legal information to decide the motion. *See* E.D. Mich. L.R. 7.1(f)(2).

It is further **ORDERED** that the parties are directed to appear as scheduled for the settlement conference on Tuesday, January 31, 2012, at 4:00 p.m.

Dated: January 30, 2012

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first class U.S. mail on January 30, 2012.

s/Tracy A. Jacobs
TRACY A. JACOBS